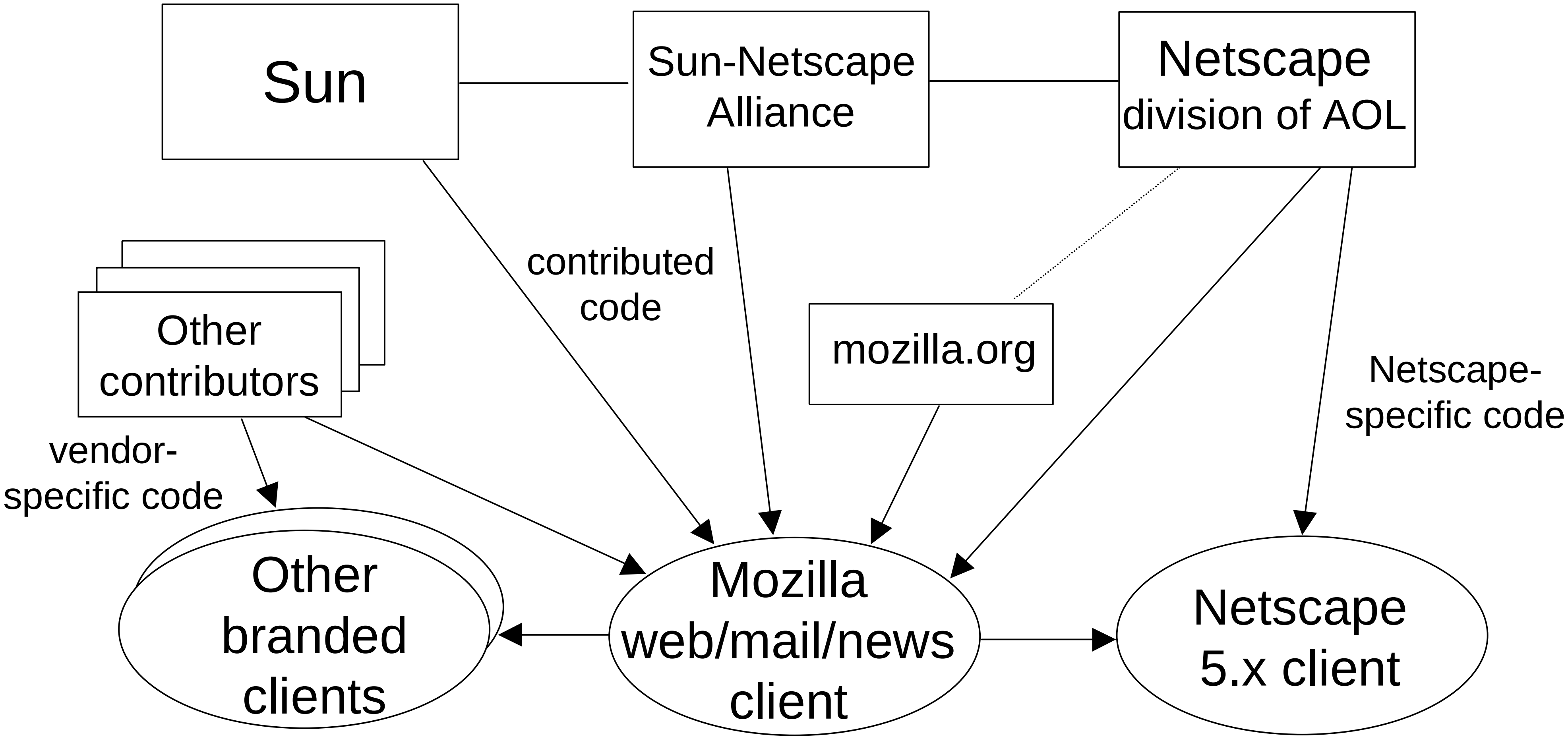
Open Source PKI Source Code for the Mozilla Internet Client

Frank Hecker
hecker@mozilla.org
frank@collab.net
301-953-2898

The Mozilla open source project



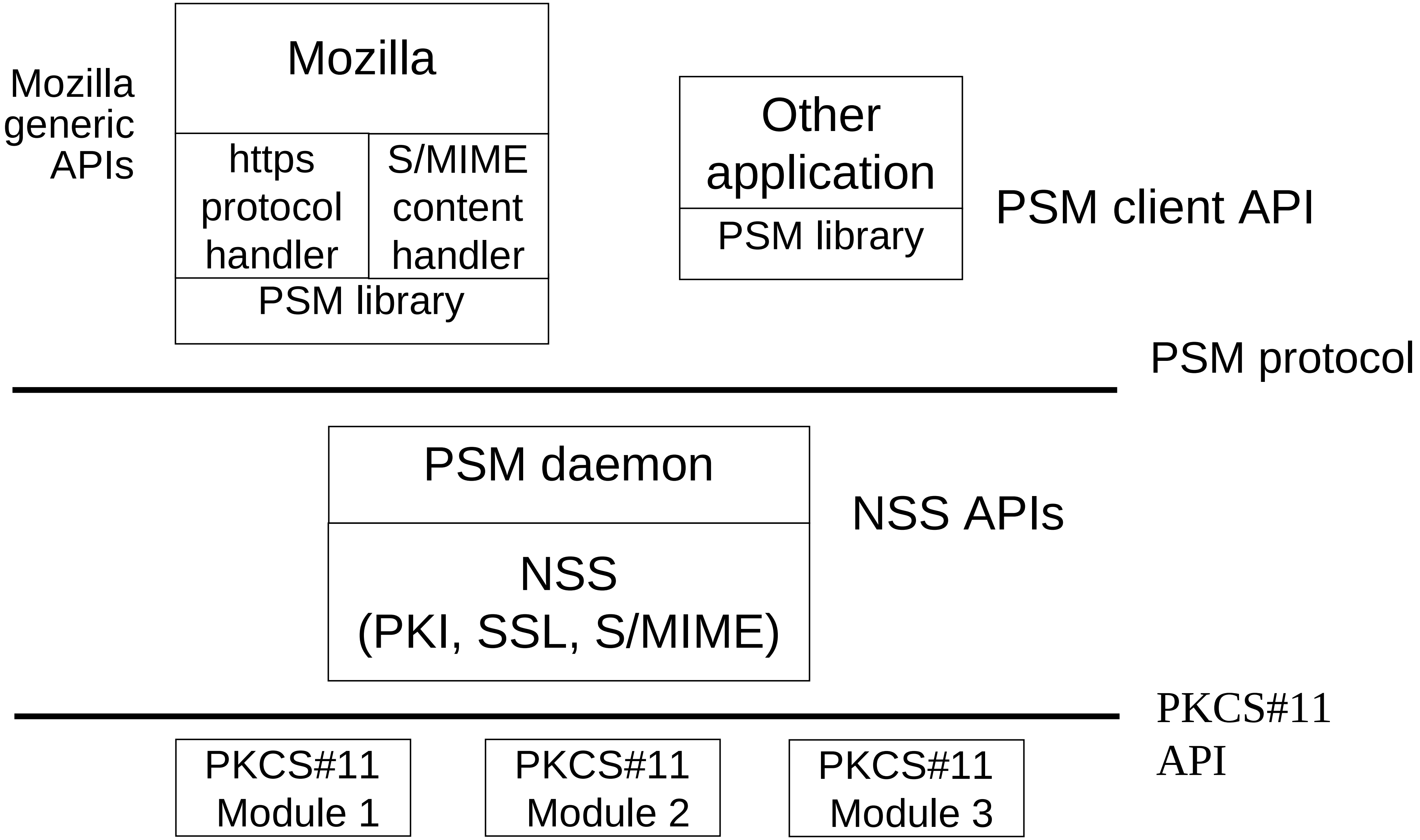
PKI/Security Code for Mozilla

- Recent relaxation of U.S. export regulations means mozilla.org can now host crypto code
- Sun/Netscape Alliance is releasing code for security and PKI functions as open source
  - code originally from Netscape security library
- What this means
  - others can directly participate in development of PKI functionality in Mozilla, Netscape 5.x, other spinoffs
  - others can reuse code for other applications, products

More details on the released code

- What is being released
  - Network Security Services (NSS)
    - cross-platform library to provide key and certificate handling/processing, SSL support, S/MIME support
  - Personal Security Manager (PSM)
    - cross-platform library/daemon to provide NSS services to multiple desktop applications: Mozilla, Netscape client, etc.
- What is *not* being released
  - core cryptographic module with RSA-licensed code
  - but PSM/NSS can use third-party PKCS#11 modules

Architecture of PSM/NSS



Mozilla generic APIs

Mozilla

https protocol handler

S/MIME content handler

PSM library

Other application

PSM library

PSM client API

PSM protocol

PSM daemon

NSS (PKI, SSL, S/MIME)

NSS APIs

PKCS#11 API

PKCS#11 Module 1

PKCS#11 Module 2

PKCS#11 Module 3

PSM/NSS Functionality

- Currently supports
  - SSLv3, S/MIMEv2 (not yet integrated into Mozilla)
  - dual key operation using standard extensions
  - CRMF/CMMF (including private key archival)
  - OCSP
- Projects for future (by Sun/Netscape or others)
  - complete set of TLS 1.0 ciphersuites
  - S/MIMEv3
  - bridge CA support

Future Possibilities

- Enhance core PSM/NSS capabilities
  - anyone welcome to contribute code to mozilla.org
- Create third-party extensions to PSM/NSS
  - add-ons can be open source or proprietary
- Provide alternatives to PSM/NSS for Mozilla
  - use Mozilla protocol handler interface for SSL/TLS
  - use content type handler interface for S/MIME
  - can hook into third-party security/PKI products to provide SSL, S/MIME, PKI functions

For More Information

- General questions:
  - http://www.mozilla.org/crypto-faq.html
- Detailed documentation and (soon) source code
  - http://www.mozilla.org/projects/security/pki
- Online discussions
  - news://news.mozilla.org/netscape.public.mozilla.crypto